Abstract

A device is provided that combines data protection for stored data with ease of use in cases where data encrypted using a public key is received and stored.

Public key encrypted data received by a data receiver module (50) is decrypted by a PKI encryption module 52 using a private key. A job controller module (51) then determines whether or not protection is necessary for this data based on processing instructions etc. for the data. When data protection is necessary, this data is encrypted by an internal key encryption module (56) and stored in HDD (16). The internal key encryption module 56 performs encryption using an internal key generated from a device serial number of a device. The internal key differs from a PKI public key in having no expiration date and not requiring updating, and can also be used to decrypt old data stored on the HDD (16).